Af/2142
IDW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Docket No. 9124

Application of

John C. Goodwin III et al.

Serial No. 09/727,338 Group Art Unit: 2142

Filed: November 29, 2000 Examiner: Vu, T.

For: **SYSTEM AND METHOD FOR A WEB WRAPPER WITH PRIVATE DATA OVERWRITING**

MS Appeal Brief-Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING
(37 CFR 1.8a)
I hereby certify that this correspondence is, on the date shown below, being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, Alexandria, VA 22313.

1-10-2005 Karen A. Church
Date Karen A. Church

Sir:

Transmitted herewith for filing is an Appeal Brief **and two copies** thereof to the Final Rejection dated August 5, 2004.

__X__ Please charge Deposit Account No. 14-0225 for the Appeal Brief fee or any other fees associated with the filing of said Appeal Brief.

__X__ Please charge any additional fees to the account of NCR Corporation, Deposit Account No. 14-0225.

Our telephone number is: (937) 445-2990.

Respectfully,

Attorney for: John C. Goodwin III et al.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 9124

Application of:

John C. Goodwin III — Art Unit: 2142

Serial No.: 09/727,338 — Examiner: T. Vu

Filed: November 29, 2000

For: PRIVATE DATA PROTECTION METHOD FOR A NETWORK KIOSK

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellants have filed a timely Notice of Appeal from the action of the Examiner, dated August 5, 2004, finally rejecting all of the claims in the present application. This Appeal Brief is filed in accordance with the provisions of 37 C.F.R. 1.192.

REAL PARTY IN INTEREST

The real party in interest is NCR Corporation.

RELATED APPEALS AND INTERFERENCES

There are no related appeals and interferences.

STATUS OF THE CLAIMS

Claims 4, 5, 7, and 8 are pending in the application.

Claims 4, 5, 7, and 8 stand rejected under 35 USC 103, as being unpatentable over Maes (6,016,476) in view of Malkin (6,317,795).

Claims 4, 5, 7, and 8 are included as Appendix A to this Appeal Brief.

STATUS OF AMENDMENTS

Appellants did not file a Response subsequent to the Final Rejection.

SUMMARY OF THE INVENTION

Claims 4, 5, 7, and 8 relate to a method of protecting private data of a user entered into a web page displayed by a network kiosk, and a network kiosk.

As embodied in independent claim 4, the invention includes

(a) displaying the web page by the kiosk (Page 6, line 14; Fig. 3, step 62);

(b) determining an address of the web page by the kiosk (Page 6, line 16; Fig. 3, step 64);

(c) determining that the address is in a table of web page addresses identifying web pages and their fields which accept the private data by the kiosk (Page 6, lines 18-24; Fig. 3, step 66);

(d) determining first fields in the one web page from the table by the kiosk (Page 6, lines 25-27; Fig. 3, step 68);

(e) determining second fields of the first fields which contain the private data by the kiosk (Page 6, lines 28-30; Fig. 3, step 70); and

(f) masking each character of the private data in the second fields with a symbol by the kiosk to prevent the private data from being seen and used by another person (Page 7, lines 3-6; Fig. 3, step 74).

As embodied in independent claim 5, the invention includes

(a) displaying the web page by the kiosk (Page 6, line 14; Fig. 3, step 62);

(b) determining an address of the web page by the kiosk (Page 6, line 16; Fig. 3, step 64);

(c) determining that the address is in a table of web page addresses identifying web pages and their fields which accept private data by the kiosk (Page 6, lines 18-24; Fig. 3, step 66);

(d) determining first fields in the one web page from the table by the kiosk (Page 6, lines 25-27; Fig. 3, step 68);

(e) determining a second field of the first fields which contains the credit card data by the kiosk (Page 6, lines 28-30; Fig. 3, step 70); and

(f) masking each character of the credit card data in the second field with a symbol by the kiosk to prevent the private data from being seen and used by another person (Page 7, lines 3-6; Fig. 3, step 74).

As embodied in independent claim 7, the invention includes

a storage medium which stores a table of web page addresses identifying web pages and their fields which accept private data of a user (Page 3, line 15; Fig. 1, block 20);

a display which displays a first web page containing the private data (Page 4, line 29; Fig. 1, block 40); and

a computer which determines an address of the first web page, determines that the address is in the table, determines first fields in the first web page from the table, determines second fields of the first fields which contain the private data, and causes the display to display a symbol for each character of the private data in the second fields to prevent the private data from being seen and used by another person (Page 3, lines 14 and 23-25; Page 4, lines 24-28; Fig. 1, block 12, 16, 32).

As embodied in dependent claim 8, the further invention includes

wherein the private data includes a credit card number and the fields include a credit card number field (Page 5, lines 29-30).

ISSUE

The issue presented by this appeal is:

Whether Claims 4, 5, 7, and 8 are patentable under 35 USC 103 over Maes (6,016,476) in view of Malkin (6,317,795).

GROUPING OF CLAIMS

The claims may be grouped together.

ARGUMENT

Maes (6,016,476) teaches a portable client personal digital assistant (PDA) for processing voice commands and biometric data to provide user verification data to an automated teller machine, point-of-sale terminal, or merchant web site. The PDA may send the user verification data in encrypted form. Maes teaches that the user verification techniques may also be used at an ATM, kiosk, or POS terminal.

Malkin (6,317,795) teaches a method of dynamically modifying multimedia content, such as multimedia streams.

I. THE REJECTION OF CLAIMS 4, 5, 7, AND 8 UNDER 35 U.S.C. §103 IS IMPROPER BECAUSE THE REFERENCES FAIL TO TEACH EACH AND EVERY ELEMENT OF APPELLANT'S CLAIMS.

The references fail to disclose a method of protecting a private data of a user from being seen and used by another while the user is using the kiosk.

Thus, with respect to claim 4, the references fail to teach or suggest the steps of

(c) determining that the address is in a table of web page addresses identifying web pages and their fields which accept the private data by the kiosk;

(d) determining first fields in the one web page from the table by the kiosk;

(e) determining second fields of the first fields which contain the private data by the kiosk; and

(f) masking each character of the private data in the second fields with a symbol by the kiosk to prevent the private data from being seen and used by another person.

With respect to claim 5, the references fail to teach or suggest the steps of

(c) determining that the address is in a table of web page addresses identifying web pages and their fields which accept private data by the kiosk;

(d) determining first fields in the one web page from the table by the kiosk;

(e) determining a second field of the first fields which contains the credit card data by the kiosk; and

(f) masking each character of the credit card data in the second field with a symbol by the kiosk to prevent the private data from being seen and used by another person.

With respect to claim 7, the references fail to teach or suggest a kiosk including

a storage medium which stores a table of web page addresses identifying web pages and their fields which accept private data of a user;

a display which displays a first web page containing the private data; and

a computer which determines an address of the first web page, determines that the address is in the table, determines first fields in the first web page from the table, determines second fields of the first fields which contain the private data, and causes the display to display a symbol for each character of the private data in the second fields to prevent the private data from being seen and used by another person.

With respect to claim 8, the references fail to teach or suggest a kiosk in which

the private data includes a credit card number and the fields include a credit card number field.

II. CONCLUSION

Appellants respectfully submit that the Examiner has failed to establish a case of obviousness and that the rejection of claims 4, 5, 7, and 8 is improper.

Appellants further submit that claims 4, 5, 7, and 8 are allowable and respectfully request that the Board reverse the rejection of claims 4, 5, 7, and 8.

Respectfully submitted,

Paul W. Martin
Attorney for Appellants
Reg. No. 34870
(937) 445-2990

Dayton, Ohio

JAN 10 2004

Appendix A

4. A method of protecting private data of a user entered into a web page displayed by a network kiosk comprising the steps of:

(a) displaying the web page by the kiosk;

(b) determining an address of the web page by the kiosk;

(c) determining that the address is in a table of web page addresses identifying web pages and their fields which accept the private data by the kiosk;

(d) determining first fields in the one web page from the table by the kiosk;

(e) determining second fields of the first fields which contain the private data by the kiosk; and

(f) masking each character of the private data in the second fields with a symbol by the kiosk to prevent the private data from being seen and used by another person.

5. A method of protecting credit card data of a customer entered into a web page displayed by a network kiosk comprising the steps of:

(a) displaying the web page by the kiosk;

(b) determining an address of the web page by the kiosk;

(c) determining that the address is in a table of web page addresses identifying web pages and their fields which accept private data by the kiosk;

(d) determining first fields in the one web page from the table by the kiosk;

(e) determining a second field of the first fields which contains the credit card data by the kiosk; and

(f) masking each character of the credit card data in the second field with a symbol by the kiosk to prevent the private data from being seen and used by another person.

7. A network kiosk comprising:

a storage medium which stores a table of web page addresses identifying web pages and their fields which accept private data of a user;

a display which displays a first web page containing the private data; and

a computer which determines an address of the first web page, determines that the address is in the table, determines first fields in the first web page from the table, determines second fields of the first fields which contain the private data, and causes the display to display a symbol for each character of the private data in the second fields to prevent the private data from being seen and used by another person.

8. The network kiosk of claim 7, wherein the private data includes a credit card number and the fields include a credit card number field.